



A GUIDE TO CYBERSECURITY RESILIENCE

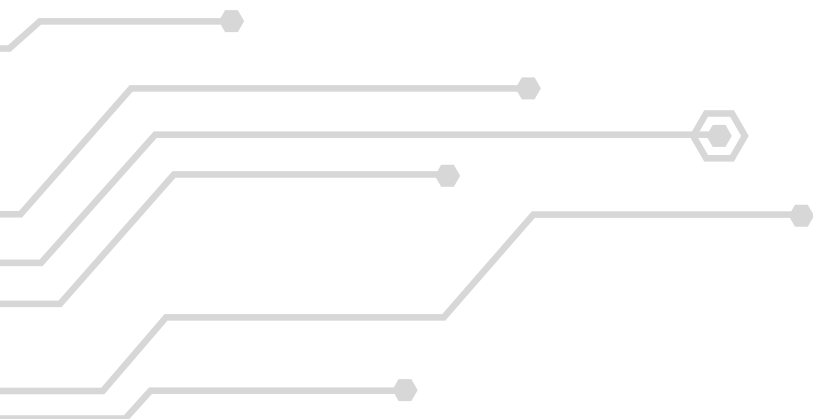


Table Of Contents

Govern Your Environment	4
Know Your Systems and Your Software	4
Manage Vulnerabilities	4
Restrict Access Privileges	5
Harden System Configurations	5
Monitor Your Logos	5
Safeguard Email and Web Browsing	6
Prepare for Malware	6
Plan to Recover Quickly	6
Protect Your Data	6
Monitor and Control Accounts	6
Security Awareness Training and Testing	7
Respond to Incidents Efficiently	7
Penetration Testing	7



Cybersecurity resilience is the ability of an organization to maintain its operations in the face of cyberattacks. It's important because it helps protect your data and systems from damage or theft and allows you to recover quickly if an attack occurs. There are many things you can do to improve your cybersecurity resilience, including:



Govern Your Environment

The first step towards resilience is to establish what your environment entails. This includes people, information technology (IT), physical resources, and other critical infrastructures that are at risk of being attacked or abused. You need to understand how these different aspects interact and be able to identify potential weak points.

Know Your Systems and Your Software

You need to understand your systems in order to protect them. Identify what information is most important, where it resides, how your systems work, and how they can be compromised. Being aware of potential risks will help you create better security measures.

Just as you need to know your systems, you also need to be aware of your software. Understand what applications and operating systems are in use, and keep them up-to-date with the latest security patches. Software vulnerabilities are a common way for attackers to gain access to networks and systems.

Manage Vulnerabilities

All systems have vulnerabilities, and it's impossible to make them 100% secure. A vulnerability could present itself in the form of a software bug, system configuration error, or even a user mistake. However, you can manage your vulnerabilities by identifying and addressing them as soon as possible. This includes applying patches and security updates, using strong passwords, installing antivirus software, and more.

Restrict Access Privileges

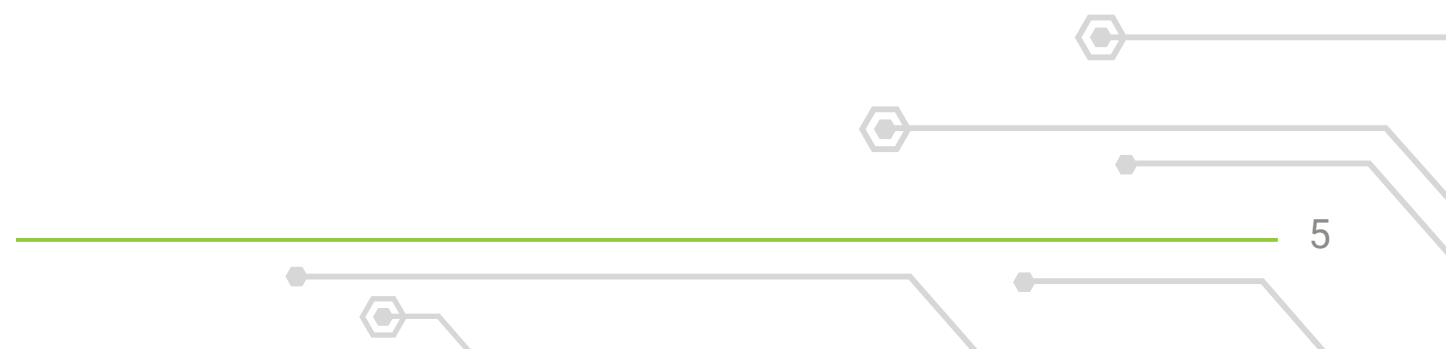
One of the best ways to reduce the impact of an attack is to restrict administrative privileges. This means that users should only be able to access systems and information they need in order to do their job. By limiting access, you can prevent unauthorized users from gaining control of your networks and systems.

Harden System Configurations

You can also harden system configurations to make them more resistant to attack. This includes disabling unnecessary services, setting appropriate permissions, using secure protocols, and many other adjustments. By taking these steps, you'll reduce vulnerabilities and make it more difficult for attackers to access your systems.

Monitor Your Logs

Logs are one of your most important tools for identifying and mitigating security incidents. They provide you with valuable information about attacks as they happen, including who is involved and how the attack was carried out. You should regularly review your logs and investigate any suspicious activity. By regularly monitoring your logs, you'll prepare for similar future threats and respond quickly to attacks.



Safeguard Email and Web Browsing

Email and web browsing are two of the most common ways for attackers to gain access to networks and systems. You can protect your email by using strong authentication methods, such as Two-Factor Authentication (2FA), and you can protect your web browsing by using a Virtual Private Network (VPN).

Prepare for Malware

Malware is one of the most common threats to cybersecurity. It comes in many different forms, and can be very difficult to detect. You can defend against malware by using antivirus software, malware removal tools, and implementing a layered approach to security.

Plan to Recover Quickly

If an attack does occur, you need to be able to recover quickly. This includes having a plan in place for responding to attacks and restoring systems and data. You should also test your recovery plan regularly to make sure it will work properly in case of an emergency.

Protect Your Data

Data is one of the most valuable assets in any organization. You need to take steps to protect your data from accidental or unauthorized access, loss, or modification. This includes using strong authentication methods, encrypting your data, and storing it in secure locations.

Monitor and Control Accounts

Attackers often use legitimate credentials to gain access to organizations. You need to be able to monitor and control accounts in order to reduce the risk of this happening. This includes using strong passwords, implementing account lockout policies, and controlling physical access.



Security Awareness Training and Testing

Awareness training can help employees avoid risky behaviors, such as phishing and other social engineering attacks. It's also a good idea to test your staff regularly by conducting security awareness tests. This will help you identify any vulnerabilities and ensure that your employees are aware of the latest threats. By assessing their knowledge, you'll be able to determine if your organization needs additional training.

Respond to Incidents Efficiently


If your organization is attacked, you need to be able to respond efficiently. This includes having a plan in place and informing the necessary people about what's happening. You should also have tools and resources in place to help you investigate and respond to attacks. It's a good idea to regularly test your response plans so that everyone knows what they should do if an attack does occur.

Penetration Testing


Penetration testing is a process that allows you to simulate an attack on your organization. It can include simulating an attack on your systems externally and internally and can help you identify vulnerabilities that can be exploited by attackers. This helps you identify vulnerabilities and determine how well your security measures are working. Penetration testing should be done regularly to help ensure the resilience of your cybersecurity defenses.

By following these tips, you can improve your cybersecurity resilience and reduce the risk of attacks. Some of the most important things you can do are train your staff, implement security policies, and regularly test your systems for vulnerabilities. By identifying potential threats before they become real problems, you can protect yourself against some of the common attacks that organizations face today.



 (801) 562-8778
Sales: (801) 859-2171

 help@itnow.net

 2436 W 700 S
Pleasant Grove, UT 84062

